WHAT IS CLAIMED IS:

1. A method, comprising:

establishing a physical channel between a sender and a receiver;

sending, from the sender to the receiver, data through a data channel;

receiving, at the receiver, the data; and

verifying, between the receiver and the sender via the physical channel, that the data is from the sender.

2. The method according to claim 1, wherein the data includes:

a key; and

a nonce.

3. The method according to claim 2, wherein the verifying comprises one of:

performing receiver-initiated verification; and

performing sender-initiated verification.

4. The method according to claim 3, wherein

the performing receiver-initiated verification comprises:

repeating, by the receiver upon receiving the data, the nonce to generated a repeating nonce;

perceiving, by the sender, the repeating nonce;

verifying the perceived repeating nonce is semantically related to the nonce sent; and

acknowledging, to the receiver, that the receiver-initiated verification is successful, if the perceived repeating nonce is verified.

the performing sender-initiated verification comprises:

repeating, by the sender after the sending, the nonce sent to the receiver to generated a repeating nonce;

perceiving, by the receiver after receiving the data, the repeating nonce;

verifying the perceived repeating nonce is the same as the nonce received; and

acknowledging, to the sender, that sender-initiated verification is successful, if the perceived repeating nonce is verified.

5. The method according to claim 2, further comprising:

storing, by the receiver, the key received from the sender as a stored key, if the verifying is successful;

sending, from the sender to the receiver, if the verifying is successful, a signed message;

receiving, at the receiver, the signed message; and

verifying the signature in the signed message using the stored key.

6. A method for a sender, comprising:

establishing a physical channel with a receiver;

sending, from the sender to the receiver, data through a data channel; and

verifying, between the sender and the receiver via the physical channel, that the receiver receives the data from the sender.

7. The method according to claim 6, wherein the data includes:

a key; and

a nonce.

8. The method according to claim 7, wherein the verifying comprises one of:

performing receiver-initiated verification, comprising;

repeating, by the receiver upon receiving the data, the nonce received from the sender to generate a repeating nonce;

perceiving, by the sender, the repeating nonce;

verifying that the perceived repeating nonce is same as the nonce sent to the receiver; and

acknowledging, to the receiver, that the receiver-initiated verification is successful, if the perceived repeating nonce is verified; and

performing sender-initiated verification, comprising:

repeating, by the sender after the sending, the nonce sent to the receiver to generate a repeating nonce;

perceiving, by the receiver upon receiving the data, the repeating nonce;

verifying that the repeating nonce is same as the nonce received; and

acknowledging, to the sender, that sender-initiated verification is successful, if the perceived repeating nonce is verified.

9. The method according to claim 7, further comprising sending, from the sender to the receiver, if the verifying is successful, a signed message.

10. A method for a receiver, comprising:

establishing a physical channel with a sender;

receiving, from the sender, data via a data channel; and

verifying, between the sender and the receiver via the physical channel, that the data, received by the receiving, is from the sender.

11. The method according to claim 10, wherein the data includes:

a key; and

a nonce.

12. The method according to claim 11, wherein the verifying comprises one of:

performing receiver-initiated verification, comprising:

repeating, by the receiver upon receiving the data, the nonce received from the sender to generate a repeating nonce;

perceiving, by the sender, the repeating nonce;

verifying that the perceived repeating nonce is same as the nonce sent to the receiver; and

acknowledging, to the receiver, that the receiver-initiated verification is successful, if the perceived nonce is verified; and

performing sender-initiated verification, comprising:

repeating, by the sender after the sending, the nonce to generate a repeating nonce;

perceiving, by the receiver upon receiving the data, the repeating nonce;

verifying that the perceived repeating nonce is same as the nonce received; and

acknowledging, to the sender, that sender-initiated verification is successful if the perceived repeating nonce is verified.

13. The method according to claim 11, further comprising:

storing, by the receiver, the key received from the sender as a stored key, if the verifying is successful;

receiving, at the receiver, a signed message; and

verifying the signature in the signed message using the stored key.

14. A system, comprising:

a sender for sending data;

a data channel through which the sender sends data;

a receiver for receiving the data sent from the sender via the data channel; and

a physical channel, established between the sender and the receiver, through which the receiver verifies that the data received by the receiver is from the sender.

15.The system according to claim 14, wherein the sender comprises:

an information generation mechanism for generating the data;

a transmitter for transmitting the data to the receiver via the data channel; and

a first verification mechanism for verifying, via the physical channel, that the data received by the receiver is from the sender.

16. The system according to claim 15, wherein the receiver comprises:

a transmission receiver for intercepting the data, sent from the sender through the data channel;

a second verification mechanism for verifying, via the physical channel and cooperating with the first verification mechanism in the sender, that the data received is from the sender; and

a key storage for storing a key included in the received data, if the verifying is successful.

17. The system according to claim 16, wherein

the sender further comprising a signed message generation mechanism for generating a signed message to be sent, after the verifying, to the receiver through the transmitter, the signed message including a signature of the sender;

the receiver further comprising a signature verification mechanism for verifying, upon receiving the signed message, the signature of the sender received through the transmission receiver.

18. A system for a sender, comprising:

an information generation mechanism for generating data;

a transmitter for transmitting the data to a receiver via a data channel; and

a verification mechanism for verifying, via a physical channel established between the sender and the receiver, that the data received by the receiver is from the sender.

19. The system according to claim 18, wherein the verification mechanism includes one of:

a receiver-initiated verification mechanism for performing a receiver-initiated verification, comprising:

repeating, by the receiver upon receiving the data, the nonce received from the sender to generate a repeating nonce;

perceiving, by the sender, the repeating nonce;

verifying that the perceived repeating nonce is same as the nonce sent to the receiver; and

acknowledging, to the receiver, that the receiver-initiated verification is successful, if the perceived nonce is verified; and

a sender-initiated verification mechanism for performing a sender-initiated verification, comprising:

an nonce repeater for generating a repeating nonce using the nonce contained in the data sent to the receiver; and

an acknowledgement perceiver for perceiving an acknowledgement from the receiver that acknowledge that the repeating nonce is same as the nonce contained in the data.

20. The system according to claim 19, further comprising a signed message generation mechanism for generating a signed message to be sent, after the verifying, to the receiver through the transmitter, the signed message including a signature of the sender.

21. A system for a receiver, comprising:

a transmission receiver for intercepting data, sent from a sender through a data channel;

a verification mechanism for verifying, via a physical channel established between the sender and the receiver, that the data received is from the sender; and

a key storage for storing a key included in the received data, if the verifying is successful.

22. The system according to claim 21, wherein the verification mechanism includes one of:

a receiver-initiated verification mechanism for performing a receiver-initiated verification, comprising:

an nonce repeater for generating a repeating nonce using the nonce contained in the data sent from the sender; and

an acknowledgement perceiver for perceiving an acknowledgement from the sender that acknowledges that the repeating nonce is same as the nonce contained in the data; and

a sender-initiated verification mechanism for performing a sender-initiated verification, comprising:

a repeating nonce perceiver for perceiving a repeating nonce, generated by the sender based on an nonce contained in the data;

an nonce verifier for verifying that the perceived repeating nonce is same as the nonce contained in the data sent from the sender; and

an acknowledgement mechanism for sending an acknowledgement, if the verifying is successful, to the sender.

23. The system according to claim 22, further comprising a signature verification mechanism for verifying the signature of the sender contained in a signed message, sent from the sender after the verifying and received by the receiver through the transmission receiver.

24. A computer-readable medium encoded with a program, the program, when executed, causing:

sending, from a sender to a receiver, data through a data channel;

receiving, at receiver, the data;

storing, by the receiver, a part of the data as a stored key, after vaerifying, via a physical channel established between the sender and the receiver, that the data received by the receiver is from the sender;

sending, from the sender to the receiver, if the verification is successful, a signed message containing a signature of the sender;

receiving, at the receiver, the signed message; and

authenticating the signature in the signed message using the stored key.

25. The medium according to claim 24, wherein the verifying includes one of:

performing receiver-initiated verification via the physical channel; or

performing sender-initiated verification via the physical channel.

26. A computer-readable medium encoded with a program for a sender, the program, when executed, causing:

sending, from a sender to a receiver, data through a data channel;

sending, from the sender to the receiver a signed message, after verifying, between the sender and the receiver via a physical channel, that the data received by the receiver is from the sender.

27. The medium according to claim 26, wherein the verifying includes one of:

performing receiver-initiated verification via the physical channel; or

performing sender-initiated verification via the physical channel.

28. A computer-readable medium encoded with a program for a receiver, the program, when executed, causing:

receiving, from a sender, data via a data channel;

storing a part of the data received from the sender as a stored key, after verifying, between the sender and the receiver via a physical channel, that the data received is from the sender;

receiving, from the sender after the verifying, a signed message containing a signature of the sender; and

authenticating the signature in the signed message using the stored key.

29. The medium according to claim 28, wherein the verifying includes one of:

performing receiver-initiated verification via the physical channel; or

performing sender-initiated verification via the physical channel.